

10/535895

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
27 mai 2004 (27.05.2004)

PCT

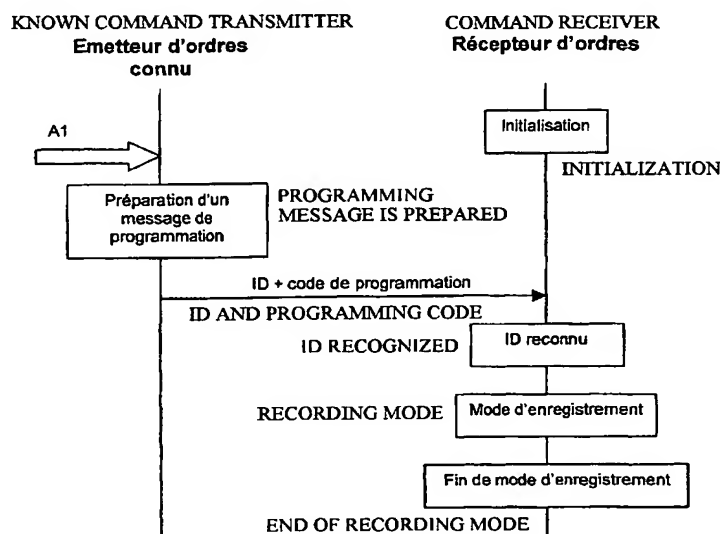
(10) Numéro de publication internationale
WO 2004/044863 A1

- (51) Classification internationale des brevets⁷ : **G08C 19/28**
- (21) Numéro de la demande internationale : **PCT/IB2003/005073**
- (22) Date de dépôt international : **7 novembre 2003 (07.11.2003)**
- (25) Langue de dépôt : **français**
- (26) Langue de publication : **français**
- (30) Données relatives à la priorité :
02/14093 12 novembre 2002 (12.11.2002) FR
- (71) Déposant (pour tous les États désignés sauf US) : **SOMFY [FR/FR]; 50, Avenue du Nouveau Monde, F-74300 Cluses (FR).**
- (72) Inventeur; et
(75) Inventeur/Déposant (pour US seulement) : **BEJEAN, Alain [FR/FR]; Le Crêt du Vernet, F-74450 Grussy (FR).**
- (74) Mandataires : **MEYLAN, Robert, M. etc.; C/O BUGNION S.A., Case Postale 375, CH-1211 Genève 12 (CH).**
- (81) États désignés (national) : **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.**
- (84) États désignés (régional) : **brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,**

[Suite sur la page suivante]

(54) Title: METHOD FOR SECURING THE RECORDING MODE OF A HOME AUTOMATION DEVICE

(54) Titre : PROCEDE DE SECURISATION DU MODE D'ENREGISTREMENT D'UN DISPOSITIF DOMOTIQUE



(57) Abstract: Disclosed is a method for securing a recording mode, which applies to a device comprising a set of at least one command transmitter that communicates with a command receiver. Said command receiver drives an element that ensures the security and/or comfort of a building and can be put in recording mode by means of one or several activation functions. The inventive method is characterized by the fact that one or several operations, at least one of which is applied to a specific secured command transmitter of the set, causes at least one activation function of the recording mode of the command receiver to be invalidated.

[Suite sur la page suivante]

WO 2004/044863 A1



FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Publiée :

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

(57) Abrégé : Le procédé de sécurisation du mode d'enregistrement s'applique à un dispositif comprenant un ensemble d'au moins un émetteur d'ordres, communiquant avec un récepteur d'ordres capable de piloter un élément assurant la sécurité et/ou le confort d'un bâtiment et susceptible d'être placé en mode d'enregistrement par une ou plusieurs fonctions d'activation. Il est caractérisé en ce qu'une ou plusieurs actions dont l'une au moins est appliquée sur un émetteur d'ordres particulier de l'ensemble, dit sécurisé, provoque l'invalidation d'au moins une fonction d'activation du mode d'enregistrement du récepteur d'ordres.

Procédé de sécurisation du mode d'enregistrement
d'un dispositif domotique.

L'invention concerne un procédé de sécurisation selon
5 le préambule de la revendication 1. L'invention se
rapporte encore à un dispositif destiné à mettre en
œuvre le procédé selon l'invention.

Par émetteur d'ordres, on entend tout élément
10 susceptible d'émettre un ordre par tout moyen et
notamment en utilisant un signal électromagnétique,
par exemple de type radiofréquence ou infrarouge, ou
en utilisant un signal électrique.

15 Dans les dispositifs permettant le pilotage d'éléments
de confort et/ou de sécurité, lorsque les émetteurs
d'ordres et les récepteurs d'ordres communiquent à
distance, il est nécessaire d'appairer ceux-ci. Cet
appariement est réalisé par la mise en œuvre d'une
20 procédure d'identification et d'enregistrement des
émetteurs, qui seront associés aux récepteurs pour
permettre la commande à distance des actionneurs
associés aux récepteurs.

25 Une telle procédure est décrite dans le brevet
EP 0 867 848. Le dispositif permettant la mise en
œuvre de cette procédure comprend deux émetteurs
possédant chacun un numéro d'identité et émettant un
signal comprenant ce numéro et un ordre. Le dispositif
30 comprend encore un récepteur muni d'une unité logique
présentant un microprocesseur et une mémoire. Le

microprocesseur est susceptible de fonctionner selon deux modes. Un premier dans lequel il permet l'exécution des ordres reçus et un deuxième dans lequel il permet l'enregistrement des numéros d'identité des émetteurs. On connaît également une
5 autre procédure du document FR 2 727 553.

Un moyen de mise en mode d'enregistrement tel qu'un bouton-poussoir situé sur le récepteur peut agir
10 directement sur le microprocesseur. Ce moyen de mise en mode d'enregistrement du microprocesseur peut également être associé à un émetteur, de telle sorte qu'au moyen de cet émetteur, il est possible de mettre le microprocesseur en mode d'enregistrement et
15 d'enregistrer le numéro d'identité d'au moins un autre émetteur. Dans le cas d'un émetteur sans fil, le numéro d'identité de cet émetteur doit être connu du microprocesseur pour pouvoir activer la mise en mode d'enregistrement. La mise en mémoire du numéro
20 d'identité de l'émetteur comprenant le moyen de mise en mode d'enregistrement peut être effectuée préalablement à l'installation, en usine par exemple. Cette mise en mémoire (ou appariement) peut également intervenir au moment de l'installation par
25 l'activation d'une fonction de mise en mode d'enregistrement du microprocesseur au niveau du récepteur comme décrit précédemment. Cette fonction n'est plus nécessairement accessible une fois le dispositif complètement installé.

Dans le cas où le moyen de mise en mode d'enregistrement est uniquement accessible sur un émetteur, des problèmes se posent lors de la perte ou du vol de cet émetteur. D'une part, il n'est plus possible d'associer ou de supprimer des émetteurs au dispositif et, d'autre part, dans le cas d'un vol, le dispositif n'est plus sécurisé.

Une solution simple permettant de résoudre ces problèmes est décrite dans le brevet EP 0 921 507. Elle consiste à commander la mise en mode d'enregistrement par une action spécifique sur l'alimentation secteur, par exemple une double coupure de courant dans un intervalle de temps réduit.

Il s'avère que cette solution permettant de faciliter l'appariement entre émetteurs et récepteurs présente un manque de sécurisation de l'accès à la mémoire des récepteurs.

En effet, si on prend l'exemple d'un portail ou d'un garage, éloigné du bâtiment principal et dont la porte est commandée par un système de commande à distance, il existe des accès non sécurisés à l'alimentation secteur, entre le portail ou le garage et le bâtiment principal. Ces accès peuvent être utilisés pour agir de manière frauduleuse sur l'alimentation secteur, de manière à mettre le récepteur du système de commande à distance en mode d'enregistrement et apparier un nouvel émetteur.

Un autre cas d'accès non sécurisé est le suivant : on trouve des interrupteurs situés au niveau du récepteur, notamment dans les systèmes d'actionneurs de portes de garage. Une action sur cet interrupteur
5 active le mode d'enregistrement du récepteur. Dans le cas d'une porte de garage laissée ouverte temporairement, l'accès à l'interrupteur est libre et celui-ci peut être utilisé à des fins frauduleuses pour l'appariement d'un nouvel émetteur.

10

Les procédés et moyens permettant le passage du dispositif en mode d'enregistrement selon l'art antérieur sont représentés aux figures 1 et 2.

15 A la figure 1, le récepteur d'ordres est initialisé lors de l'installation du dispositif. La phase d'initialisation comprend également les procédures d'appariement d'un ou plusieurs émetteurs au cours desquelles le récepteur reçoit le numéro d'identité du
20 ou des émetteurs et les stocke en mémoire.

Pour mettre le récepteur en mode d'enregistrement, un utilisateur effectue, sur un émetteur déjà connu par le récepteur d'ordres, une action A1 de mise en mode
25 d'enregistrement, par exemple par appui sur un bouton spécifique prévu sur cet émetteur. L'émetteur prépare et envoie un message de programmation contenant son numéro d'identité ID et un code de programmation permettant le passage du récepteur en mode
30 d'enregistrement.

Lors de la réception du message provenant de l'émetteur d'ordres, le récepteur vérifie si le numéro d'identité ID reçu est en mémoire. Si tel est le cas, le récepteur d'ordres est prêt à recevoir des messages de commande de l'actionneur de la part de l'émetteur. Dans le cas où un code de programmation est reçu, le récepteur passe en mode d'enregistrement. Il est alors possible d'apparier de nouveaux émetteurs ou d'en supprimer. La sortie du mode d'enregistrement est consécutive, soit au déroulement d'une temporisation, soit à une nouvelle commande de l'utilisateur.

Une autre procédure de mise en mode d'enregistrement du récepteur, connue de l'art antérieur, est représentée à la figure 2. Cette procédure est initiée par une action A2 de l'utilisateur sur un moyen de mise en mode d'enregistrement, associé directement au récepteur ou par une action spécifique sur l'alimentation secteur.

Du brevet JP 2001032587, on connaît une solution proposant d'utiliser des unités indépendantes pour reprogrammer le système gérant l'ouverture des portes d'un véhicule. Cette solution a pour but une sécurisation du système par rapport au vol des émetteurs, mais ne résout pas le problème de l'accès aux moyens fixes de mise en mode d'enregistrement dans les procédures d'appariement entre émetteurs et récepteurs.

30

Le but de l'invention est de fournir un procédé permettant de résoudre les problèmes précités et d'améliorer les procédés de l'art antérieur. En particulier, l'invention se propose de mettre en œuvre
5 un procédé permettant de sécuriser l'accès aux fonctions d'enregistrement des récepteurs d'ordres dans le cadre de dispositifs assurant la sécurité et/ou le confort d'un bâtiment. L'invention se propose encore de réaliser un dispositif permettant de mettre
10 en œuvre ce procédé.

Le procédé selon l'invention est caractérisé par la partie caractérisante de la revendication 1.

Différents modes d'exécution de ce procédé sont définis par les revendications dépendantes 2 à 7.

15 La revendication indépendante 8 définit un dispositif permettant la mise en œuvre de ce procédé.

Les revendications dépendantes 9 et 10 définissent des modes de réalisation du dispositif selon l'invention.

20 On peut donc distinguer trois types d'émetteurs qui peuvent communiquer avec le récepteur d'ordres du dispositif :

- un émetteur simple de commande (montée/descente, ouverture/fermeture),
- 25 - un émetteur de programmation (commande et fonction d'activation du mode d'enregistrement du récepteur),

- un émetteur d'ordres sécurisé (commande optionnelle, fonctions d'activation du mode d'enregistrement et d'invalidation).

Les deux fonctions principales de l'émetteur d'ordres
5 sécurisé sont donc la mise en mode d'enregistrement du
récepteur et l'invalidation des fonctions d'activation
du mode d'enregistrement. Ces fonctions principales
sont activées soit par des actions différentes, soit
par une action commune sur un ou plusieurs émetteurs
10 présentant des moyens de mise en mode d'enregistrement
et des moyens d'invalidation des fonctions
d'activation.

De manière préférée, les émetteurs d'ordres sécurisés
comportent des moyens sans fil de communication à
15 distance avec le récepteur d'ordres.

Les émetteurs d'ordres sécurisés présentent de
préférence deux dimensions sensiblement égales aux
dimensions normalisées d'une feuille de papier afin de
pouvoir être conservés facilement dans un endroit sûr
20 tel qu'un coffre. Ils peuvent également être munis de
moyens visuels tels que des étiquettes afin d'indiquer
à l'utilisateur à quels dispositifs ils sont associés.

Le dispositif comporte un émetteur dont les fonctions
25 sont la mise en mode d'enregistrement du dispositif et
l'envoi d'un code de sécurisation et un récepteur tel
que la réception du code de sécurisation provoque
l'invalidation du ou des autres moyens de mise en mode
d'enregistrement.

Le dispositif peut être utilisé de façon préventive. Une fois que les appariements souhaités entre émetteurs et récepteurs ont été effectués, on peut transmettre au récepteur, grâce à l'émetteur sécurisé, 5 le code de sécurisation de manière à limiter ses possibilités de mise en mode d'enregistrement.

L'émetteur sécurisé ne comporte pas nécessairement de fonction de commande de l'actionneur. De cette 10 manière, il peut consister en un émetteur simple, de moindre coût et plus facile à ranger dans un endroit sûr. Cependant, on peut prévoir un émetteur sécurisé associé à un émetteur plus évolué, qui pourrait être éventuellement fixé à l'intérieur de l'habitat.

15 L'émetteur sécurisé peut permettre une invalidation unique, c'est à dire une annulation irréversible du ou des moyens de mise en mode d'enregistrement. Il peut être prévu également sur l'émetteur sécurisé une 20 fonction de réactivation des différents moyens de mise en mode d'enregistrement. Dans les deux cas, l'émetteur sécurisé peut être réutilisé pour la fonction d'activation du mode d'enregistrement du récepteur.

25 Il peut également être prévu une fonction d'effacement des numéros d'identité déjà enregistrés, par exemple par une manœuvre spéciale sur l'émetteur sécurisé.

Le dessin annexé représente, à titre d'exemples, plusieurs modes d'exécution du procédé selon l'invention.

5 La figure 1 est un ordinogramme d'un procédé de mise en mode d'enregistrement selon l'art antérieur.

La figure 2 est un ordinogramme d'un autre procédé de mise en mode d'enregistrement selon l'art antérieur.

10

La figure 3 est un ordinogramme d'un premier mode d'exécution du procédé de sécurisation du mode d'enregistrement lors d'une première utilisation de l'émetteur d'ordres sécurisé.

15

Les figures 4a et 4b sont deux parties d'un ordinogramme d'un deuxième mode d'exécution du procédé de sécurisation du mode d'enregistrement lors d'une première utilisation de l'émetteur d'ordres sécurisé.

20

La figure 5 est un ordinogramme du premier mode d'exécution du procédé de sécurisation du mode d'enregistrement lors d'une utilisation ultérieure de l'émetteur d'ordres sécurisé.

25

La figure 6 est un schéma représentant un émetteur d'ordres et un récepteur d'ordres.

30 Le dispositif représenté à la figure 6 permet la mise en œuvre du procédé selon l'invention. Il comprend un récepteur d'ordres 10 et un ensemble d'émetteurs

d'ordres 20. Pour simplifier, un seul émetteur a été représenté à la figure 6.

Le récepteur d'ordres 10 comprend un module récepteur
5 12 raccordé, d'une part, à un dispositif de couplage
11 et, d'autre part, à une unité de traitement 13 de
type microcontrôleur pilotant un équipement 14 tel
qu'une porte, un volet roulant ou une installation
d'alarme. Le récepteur d'ordre peut également
10 comprendre une interface de commande 15 de type
bouton-poussoir. Le récepteur d'ordres est relié à une
alimentation secteur 17.

L'unité de traitement 13 comprend une zone de mémoire
15 16 destinée à contenir des programmes de
fonctionnement du récepteur 10 et les numéros
d'identité des émetteurs d'ordres 20 desquels le
récepteur 10 est susceptible de recevoir des ordres.

20 Chaque émetteur d'ordres 20 comprend un module
émetteur 22 raccordé, d'une part, à un dispositif de
couplage 21 et, d'autre part, à une unité de
traitement 23 de type microcontrôleur, et une
interface de commande 24 de type clavier. Chaque
25 émetteur d'ordres 20 contient son numéro d'identité
dans une zone de mémoire 26 de l'unité de traitement
23.

Les émetteurs d'ordres sont susceptibles de
30 transmettre des ordres par le biais d'ondes
électromagnétiques, de type radio ou de type

infrarouge ou encore par le biais de liaisons filaires.

Les communications entre émetteurs d'ordres et
5 récepteurs d'ordres peuvent être bidirectionnelles.
Dans ce cas, émetteurs et récepteurs sont munis de modules « émetteur-récepteur ».

Les émetteurs d'ordres, ou au moins certains d'entre
10 eux, peuvent par une action ou une série d'actions de l'utilisateur faire passer le récepteur dans un mode d'enregistrement dans lequel il est possible de modifier la liste des émetteurs qui lui sont appariés par ajout ou par suppression de ceux-ci.

15 Parmi les émetteurs d'ordres, un émetteur particulier dit émetteur d'ordres sécurisé permet d'invalidiser certaines fonctions de mise en mode d'enregistrement du récepteur.

20 La figure 3 représente un premier mode d'exécution du procédé de fonctionnement du dispositif lors d'une première utilisation de l'émetteur d'ordres sécurisé.

25 La première action consiste à mettre le récepteur en mode d'enregistrement par une commande de type A1 (par un émetteur d'ordre) ou de type A2 (directement au niveau du récepteur ou sur l'alimentation secteur). L'utilisateur peut alors activer une commande de
30 lancement de programme sécurisé A3 qui provoque l'envoi d'un message contenant le numéro d'identité ID

de l'émetteur sécurisé BPS, pour l'apparier avec le récepteur, éventuellement un code de programmation et le code de programmation sécurisé.

- 5 Le récepteur reconnaît le numéro d'identité ID de l'émetteur.

La réception du code de programmation sécurisé provoque le lancement d'un programme de sécurisation
10 associé et, par conséquent, l'invalidation des moyens de mise en mode d'enregistrement de type A1 et/ou de type A2.

Cette invalidation des moyens de mise en mode
15 d'enregistrement peut consister en un changement d'état de mémoires binaires associées au récepteur et validant ou non les moyens de mise en mode d'enregistrement par les différents émetteurs.

- 20 Le récepteur peut alors activer un signal de fin de procédure signifiant à l'utilisateur que les moyens de mise en mode d'enregistrement ont été invalidés. Ce signal peut également être émis par l'émetteur d'ordres sécurisé après réception d'un message émis
25 par le récepteur, dans le cas où la communication est bidirectionnelle.

Dans un tel mode d'exécution, les fonctions de mise en mode d'enregistrement et d'invalidation peuvent être
30 soit communes à une même action sur l'émetteur d'ordres sécurisé, soit différenciées.

Dans le premier cas, la réception du code de programmation n'affecte pas le récepteur qui se trouve déjà en mode d'enregistrement. Eventuellement, dans le cas d'une fin de mode d'enregistrement consécutive au déroulement d'une temporisation, cette dernière peut
5 être réinitialisée suite à la réception d'un code de programmation par le récepteur d'ordres.

Dans le deuxième cas, le code de programmation n'est
10 pas envoyé par l'émetteur d'ordres sécurisé.

Les figures 4a et 4b représentent un deuxième mode d'exécution du procédé de fonctionnement du dispositif lors d'une première utilisation de l'émetteur d'ordres
15 sécurisé, lorsque les fonctions d'identification de l'émetteur d'ordres sécurisé et la commande d'invalidation sont découplées. Dans ce cas, deux actions spécifiques doivent être effectuées sur l'émetteur d'ordres sécurisé par l'utilisateur. Ces
20 deux actions peuvent être décalées dans le temps.

La figure 4a représente le procédé d'appariement de l'émetteur d'ordres sécurisé. Une première action A4, effectuée alors que le récepteur a été préalablement
25 mis en mode d'enregistrement, permet d'apparier l'émetteur d'ordres sécurisé et le récepteur d'ordres. Elle provoque l'envoi uniquement du numéro d'identité ID de l'émetteur d'ordres sécurisé et sa réception et son stockage par le récepteur d'ordres.

La figure 4b représente le fonctionnement de l'émetteur d'ordres sécurisé une fois connu du récepteur. Une seconde action A5 provoque l'envoi d'un message contenant le numéro d'identité ID de l'émetteur d'ordres sécurisé, éventuellement un code de programmation et un code de programmation sécurisé. Le numéro d'identité de l'émetteur ayant été enregistré dans le récepteur lors de l'action précédente, celui-ci est reconnu par le récepteur et le code de programmation sécurisé est stocké en mémoire provoquant le lancement du programme de sécurisation associé à ce code. Les moyens de mise en mode d'enregistrement de type A1 et/ou de type A2 sont par conséquent invalidés.

15

Lorsque les fonctions de mise en mode d'enregistrement et d'invalidation sont communes à un type d'action sur l'émetteur d'ordres sécurisé, la réception des codes de programmation entraîne de façon sensiblement simultanée la mise en mode d'enregistrement du récepteur et l'invalidation des fonctions d'activation du mode d'enregistrement.

De manière générale, la fonction d'invalidation implique l'invalidation des fonctions d'activation du mode d'enregistrement, à l'exception de la fonction d'activation du mode d'enregistrement de l'émetteur d'ordres sécurisé.

Dans le cas où les deux fonctions de mise en mode d'enregistrement et d'invalidation doivent être

activées par deux types d'actions différenciés, une action entraîne une mise en mode d'enregistrement du récepteur d'ordre, de la manière représentée sur la figure 1 et une action entraîne l'envoi du numéro d'identité ID de l'émetteur d'ordres sécurisé et du code de programmation sécurisé uniquement. Ainsi, seule la fonction d'invalidation est activée.

Comme dans le mode d'exécution précédent, le récepteur peut alors activer un signal de fin de procédure signifiant à l'utilisateur que les moyens de mise en mode d'enregistrement ont été invalidés. Ce signal peut également être émis par l'émetteur d'ordres sécurisé après réception d'un message émis par le récepteur, dans le cas où la communication est bidirectionnelle.

Il existe plusieurs cas pour lesquels l'émetteur d'ordres sécurisé est activé alors que son numéro d'identité ID est déjà connu du récepteur :

- Lors d'une première utilisation, dans le cas de la figure 4b, si l'émetteur d'ordres sécurisé a été apparié au récepteur d'ordres sans qu'il ne soit envoyé simultanément de code de programmation ou de code de programmation sécurisé,
- soit lors d'une utilisation ultérieure de l'émetteur d'ordres sécurisé, pour la mise en mode d'enregistrement du dispositif,

- soit s'il est prévu des moyens pour réactiver les moyens de mise en mode d'enregistrement originels.

5 La figure 5 représente le procédé mis en œuvre lorsque l'émetteur d'ordres est connu du récepteur, lors d'une utilisation ultérieure. Par une action A3 sur l'émetteur sécurisé, l'utilisateur provoque l'envoi d'un message contenant le numéro d'identité ID de
10 l'émetteur d'ordres sécurisé, éventuellement le code de programmation, et le code de programmation sécurisé. Le récepteur reçoit ce message, reconnaît le numéro d'identité ID de l'émetteur d'ordres sécurisé et mémorise le code de programmation sécurisé.

15

Il est possible de prévoir un test de la validité des moyens de mise en mode d'enregistrement par exemple en testant l'état de mémoires binaires. Si les moyens de mise en mode d'enregistrement sont valides (test
20 positif +), le récepteur les invalide avant d'enregistrer cette configuration. Il passe alors éventuellement en mode d'enregistrement. Si les moyens de mise en mode d'enregistrement sont déjà invalidés (test négatif -), le récepteur peut alors passer en
25 mode d'enregistrement, de manière à pouvoir initier une procédure d'appariement.

Ce test est facultatif et évite uniquement de retransmettre un ordre d'invalidation vers des moyens
30 de mise en mode d'enregistrement déjà invalidés, notamment dans le cas où une seule action sur

l'émetteur d'ordre sécurisé entraîne à la fois la mise en mode d'enregistrement du récepteur et l'invalidation d'autres fonctions d'activation de ce mode d'enregistrement.

- 5 Bien entendu, dans tous les modes d'exécutions de l'invention, la transmission d'un numéro d'identité peut être remplacée par toute autre méthode d'identification, comme par exemple une méthode de Challenge.
- 10 De même, on peut aussi prévoir que le code de programmation sécurisé soit remplacé par une partie générique du numéro d'identité d'un émetteur d'ordres sécurisé, qui caractérise l'émetteur d'ordres sécurisé et la fonction d'invalidation associée.

Revendications :

1. Procédé de sécurisation du mode d'enregistrement d'un dispositif comprenant un ensemble d'au moins un émetteur d'ordres (20), communiquant avec un
5 récepteur d'ordres (10) capable de piloter un élément (14) assurant la sécurité et/ou le confort d'un bâtiment et susceptible d'être placé en mode d'enregistrement par une ou plusieurs fonctions d'activation, caractérisé en ce qu'une ou
10 plusieurs actions dont l'une au moins est appliquée sur un émetteur d'ordres particulier de l'ensemble, dit sécurisé, provoque l'invalidation d'au moins une fonction d'activation du mode d'enregistrement du récepteur d'ordres.
- 15 2. Procédé de sécurisation selon la revendication 1, caractérisé en ce que les actions sont menées de manière successive ou simultanée sur au moins un émetteur d'ordres sécurisé et sur au moins un autre émetteur d'ordres.
- 20 3. Procédé de sécurisation selon la revendication 1 ou 2, caractérisé en ce que la ou les actions sur l'émetteur d'ordres sécurisé activent le mode d'enregistrement du récepteur.
- 25 4. Procédé de sécurisation selon l'une des revendications 1 à 3, caractérisé en ce que la ou les actions sur l'émetteur d'ordres sécurisé invalident les fonctions d'activation du mode

d'enregistrement à l'exception de celles des émetteurs d'ordres sécurisés.

5. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce que
5 l'invalidation de la fonction d'activation est irréversible.
6. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce que
10 l'invalidation de la fonction d'activation est temporaire.
7. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce qu'une action sur un émetteur d'ordres sécurisé provoque, dans la mémoire du récepteur,
15 l'effacement des numéros d'identité d'au moins certains émetteurs.
8. Dispositif destiné à mettre en œuvre le procédé selon l'une des revendications 1 à 7, caractérisé en ce qu'il comprend au moins un émetteur d'ordres
20 sécurisé, et éventuellement d'autres émetteurs d'ordres (20), communiquant avec un récepteur d'ordres (10) capable de piloter un élément (14) assurant la sécurité et/ou le confort d'un bâtiment.
- 25 9. Dispositif selon la revendication 8, caractérisé en ce que les émetteurs d'ordres sécurisés

comportent des moyens sans fil de communication à distance avec le récepteur d'ordres (10).

- 5 10. Dispositif selon la revendication 8 ou 9, caractérisé en ce que les émetteurs d'ordres sécurisés présentent deux dimensions sensiblement égales aux dimensions normalisées d'une feuille de papier.

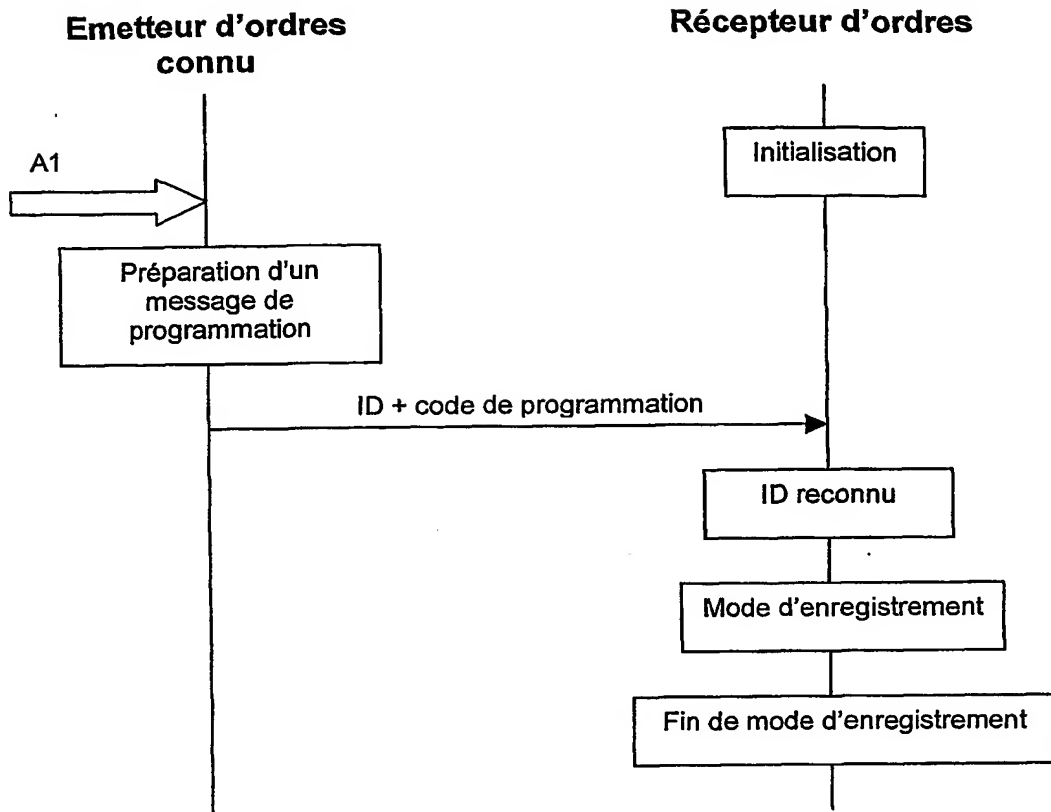


Fig. 1 (Art antérieur)

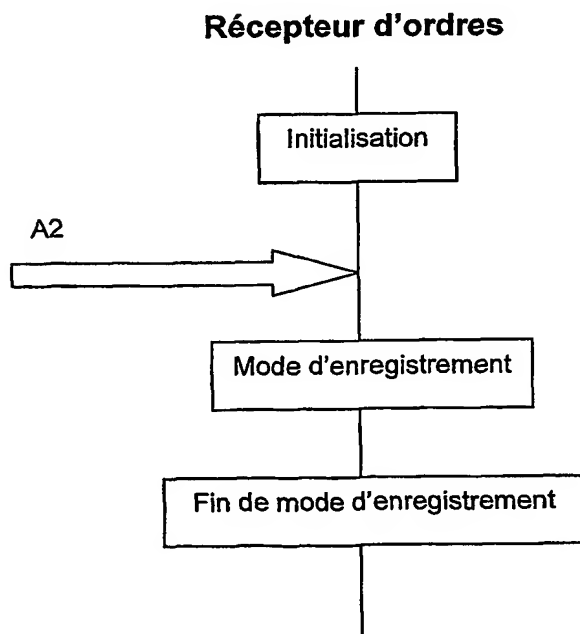


Fig. 2 (Art antérieur)

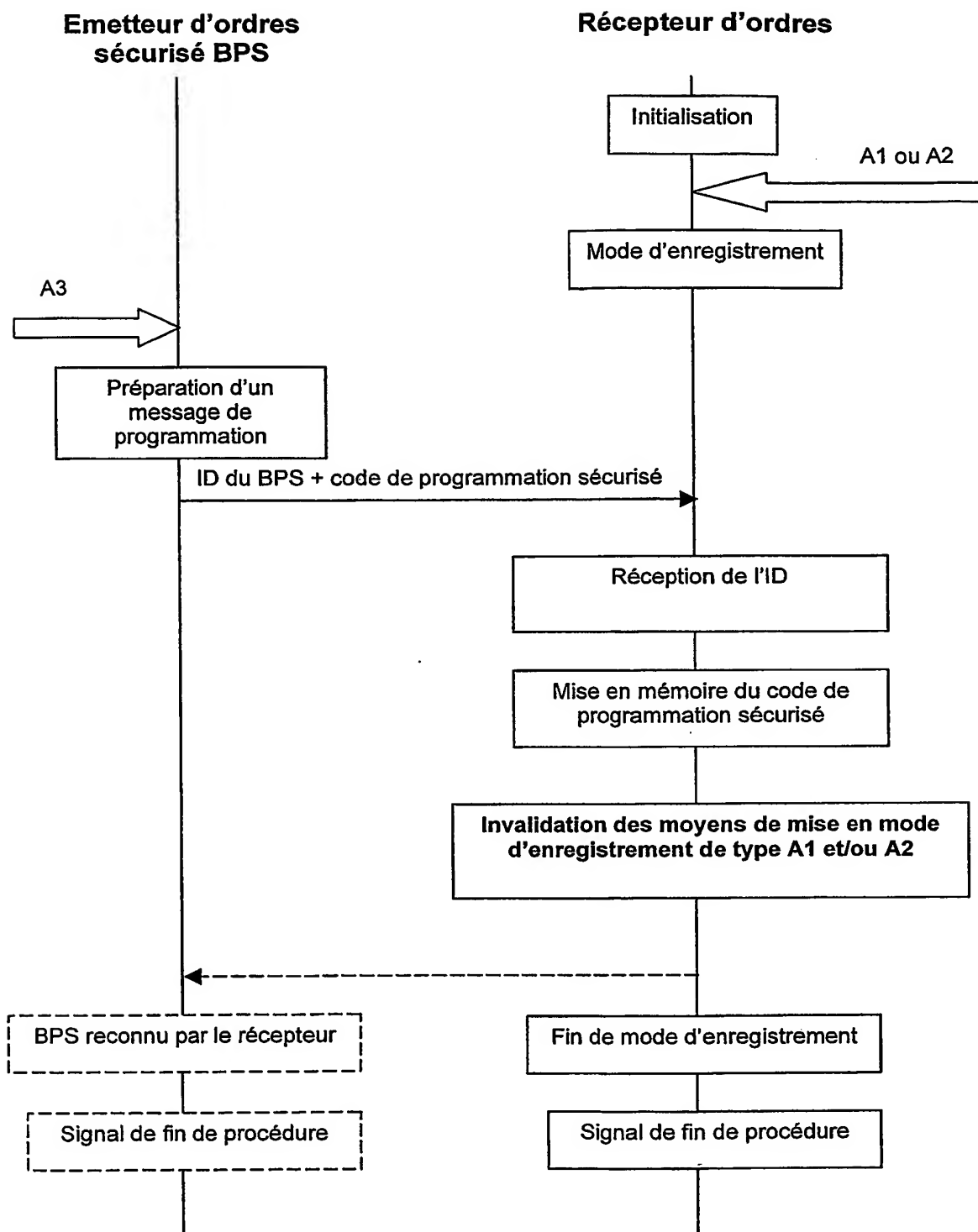
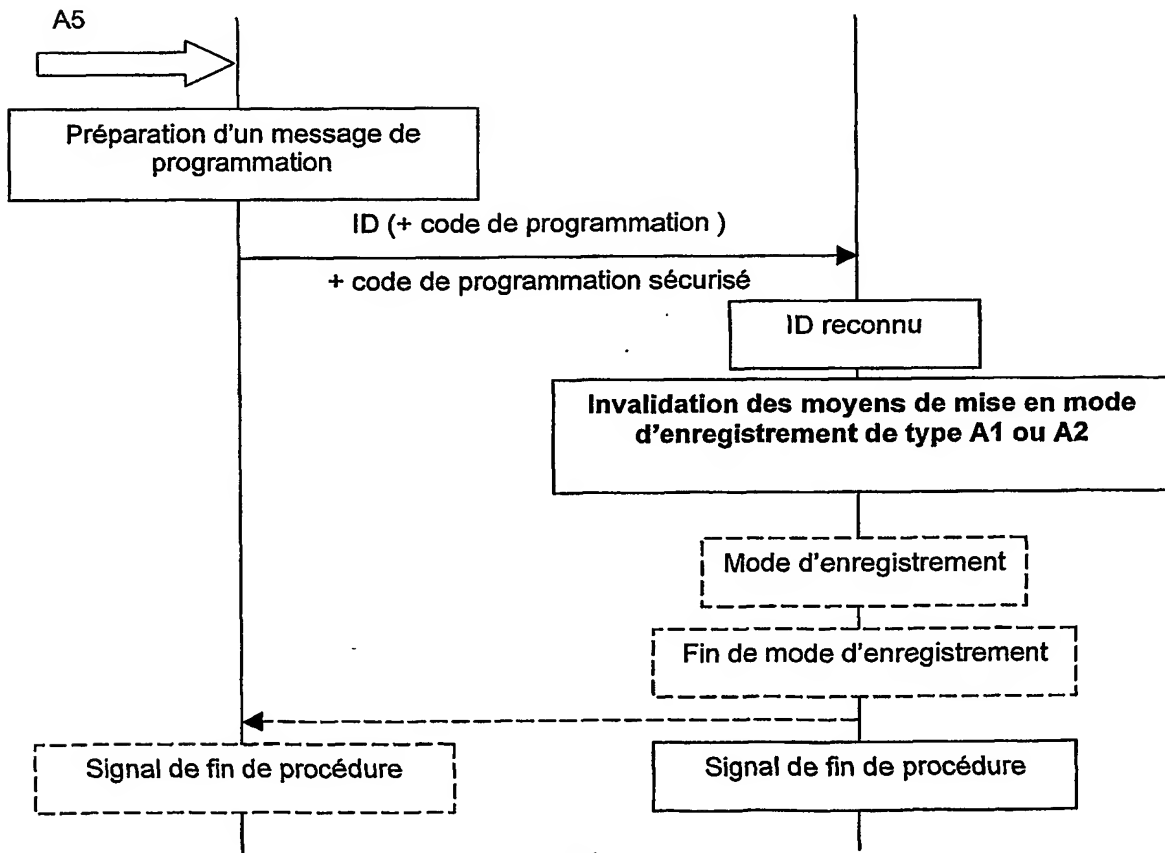
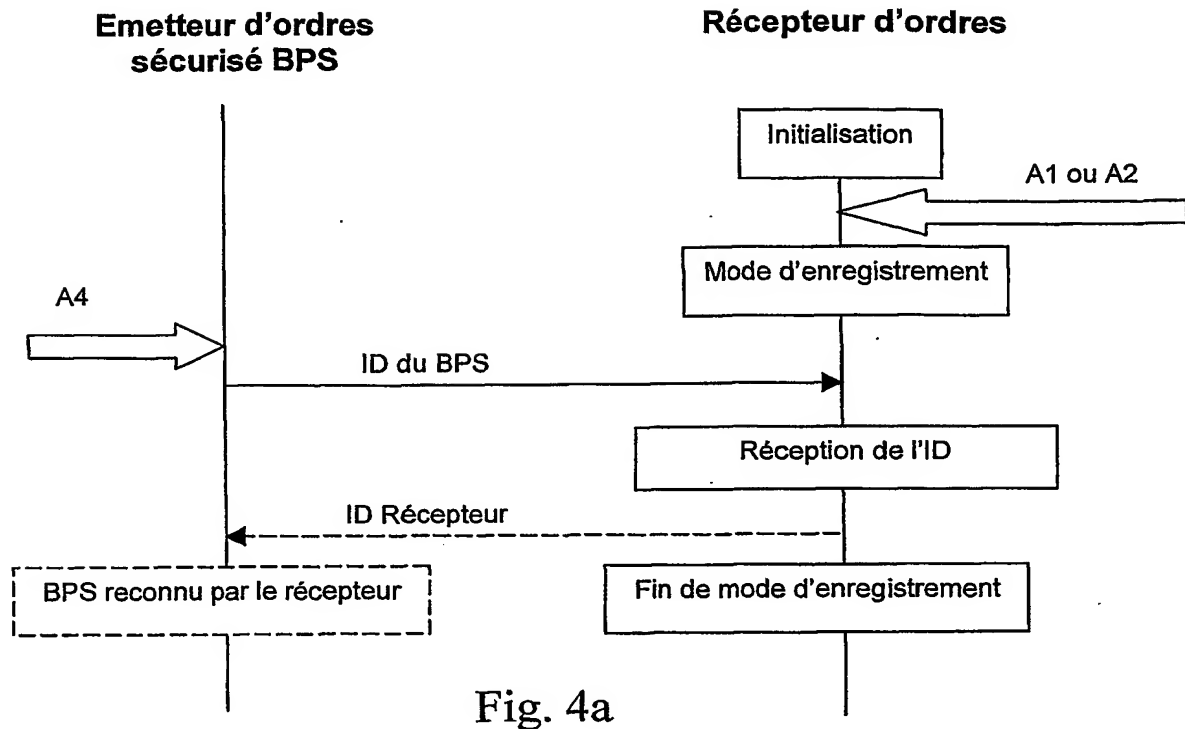


Fig. 3



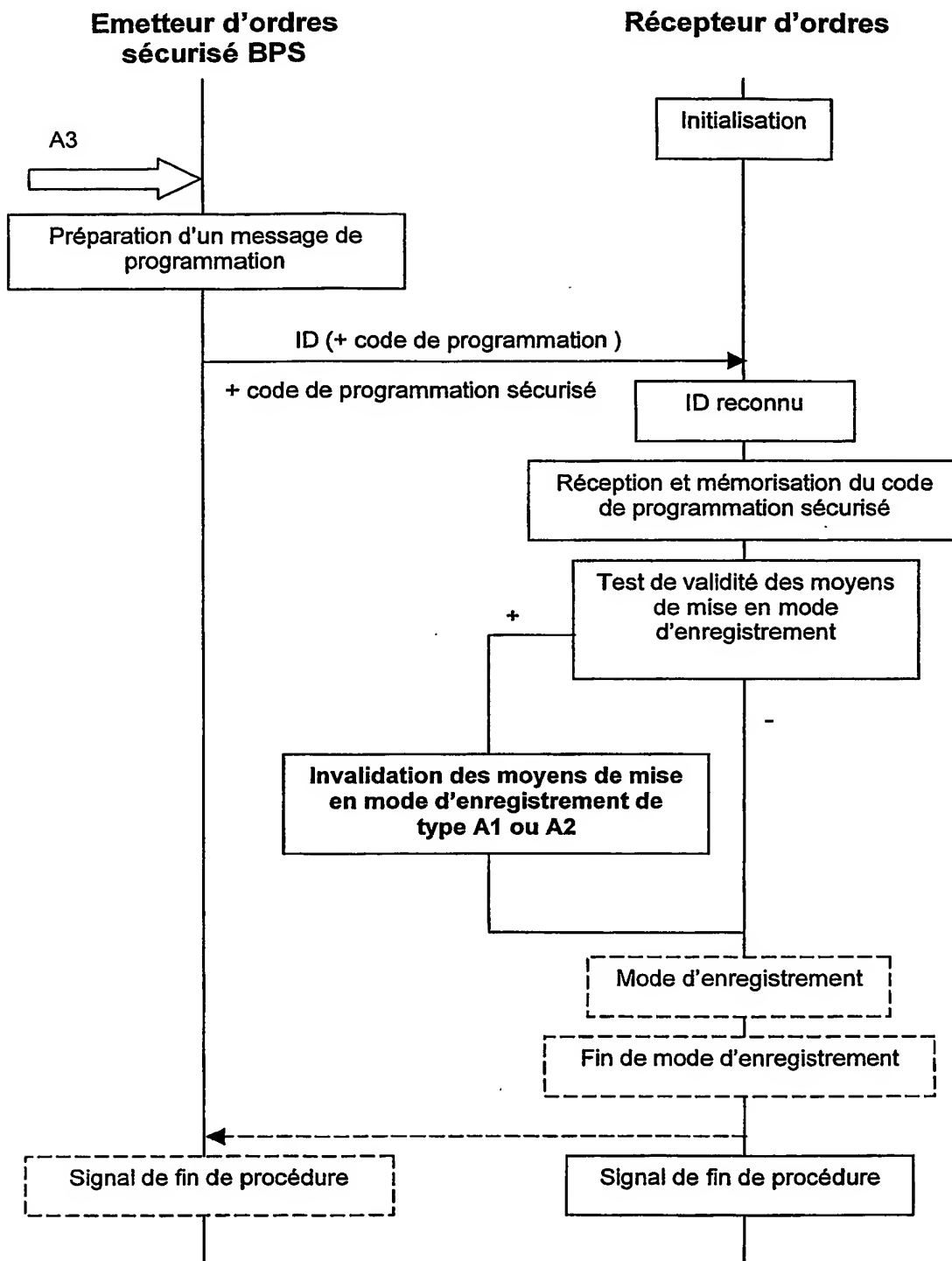


Fig. 5

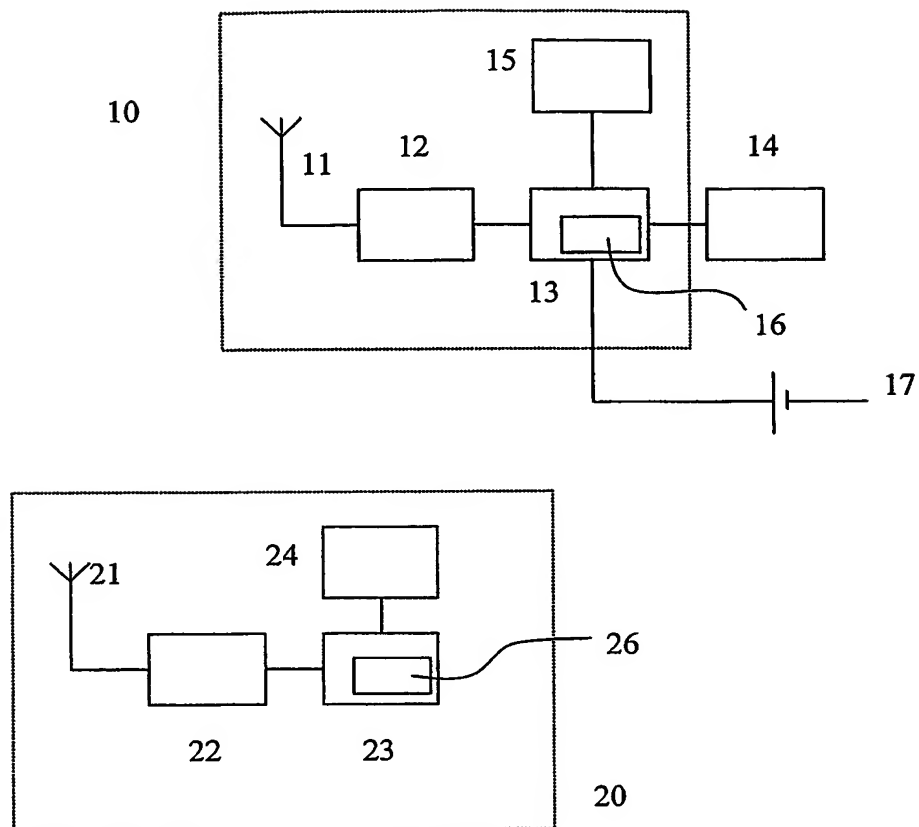


Fig.6

Internat	Application No
PCT	03/05073

According to International Patent Classification (IPC) or to both national classification and IPC

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G08C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

EPO-Internal, WPI Data, PAJ, INSPEC

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 727 553 A (LEGRAND SA) 31 May 1996 (1996-05-31) page 4, line 1 -page 7, line 11 -----	1-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

30 March 2004

07/04/2004

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

LOPEZ PEREZ M-C.

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT 03/05073

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
FR 2727553	A	31-05-1996	FR 2727553 A1	31-05-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/IB 03/05073

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G08C19/28

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G08C

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	FR 2 727 553 A (LEGRAND SA) 31 mai 1996 (1996-05-31) page 4, ligne 1 -page 7, ligne 11 -----	1-10

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

30 mars 2004

Date d'expédition du présent rapport de recherche internationale

07/04/2004

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

LOPEZ PEREZ M-C.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/ 03/05073

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2727553	A	31-05-1996	FR 2727553 A1	31-05-1996